(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
13. Januar 2005 (13.01.2005)

PCT

(10) Internationale Veröffentlichungsnummer
WO 2005/004381 A1

(51) Internationale Patentklassifikation[7]: H04L 9/08, G06F 7/58

(21) Internationales Aktenzeichen: PCT/EP2004/007378

(22) Internationales Anmeldedatum:
6. Juli 2004 (06.07.2004)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
103 30 643.9 7. Juli 2003 (07.07.2003) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **SIEMENS AKTIENGESELLSCHAFT** [DE/DE]; Wittelsbacherplatz 2, 80333 München (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: **DÖBRICH, Udo** [DE/DE]; Hornisgrindestr. 3, 76307 Karlsbad (DE). **HEIDEL, Roland** [DE/DE]; Guttenbergstr. 31, 76870 Kandel (DE). **LINZENKIRCHNER, Edmund** [DE/DE]; Mozartstr. 4h, 76344 Eggenstein-Leopoldshafen (DE).

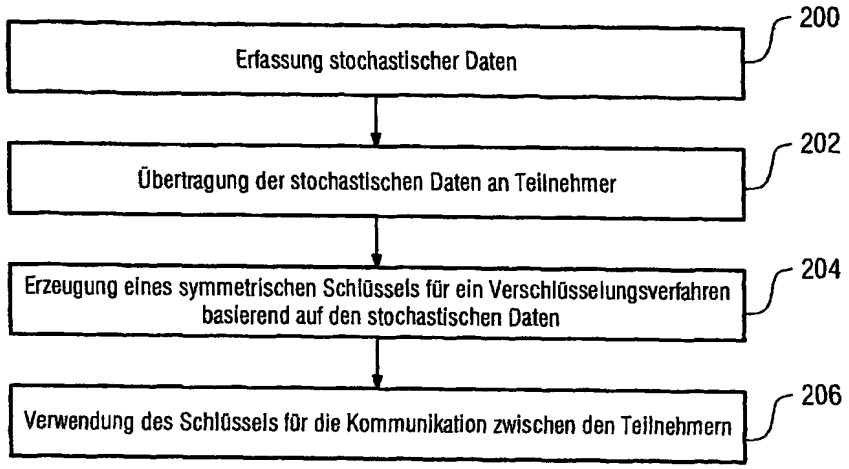
(74) Gemeinsamer Vertreter: **SIEMENS AKTIENGESELLSCHAFT**; Postfach 22 16 34, 80506 München (DE).

(81) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare nationale Schutzrechtsart)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM,

[Fortsetzung auf der nächsten Seite]

(54) Title: METHOD FOR ENCODED DATA TRANSMISSION VIA A COMMUNICATION NETWORK

(54) Bezeichnung: VERFAHREN ZUR VERSCHLÜSSELTEN DATENÜBERTRAGUNG ÜBER EIN KOMMUNIKATIONSNETZ



200. COLLECTION OF STOCHASTIC DATA
202. TRANSMISSION OF STOCHASTIC DATA TO SUBSCRIBERS
204. PRODUCTION OF A SYMMETRICAL KEY FOR AN ENCODING METHOD BASED ON THE STOCHASTIC DATA
206. USE OF KEY FOR COMMUNICATION BETWEEN SUBSCRIBERS

(57) Abstract: The invention relates to a method for data transmission, comprising the following steps: first data from a stochastic process (114) is inputted into at least a first and a second subscriber (102, 104; 402, 404; 502, 504, 506, 508, 510, 512, 516) of a communication network (100, 106; 400, 406; 500, 514, 518); and a symmetrical key (S1, S2) is produced on the basis of the first data in both the first and the second subscriber, and stored in the same, for an encoded data transmission between said subscribers.

[Fortsetzung auf der nächsten Seite]

WO 2005/004381 A1

TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare regionale Schutzrechtsart)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Veröffentlicht:

— *mit internationalem Recherchenbericht*

— *vor Ablauf der für Änderungen der Ansprüche geltenden Frist; Veröffentlichung wird wiederholt, falls Änderungen eintreffen*

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

(57) Zusammenfassung: Die Erfindung betrifft ein Verfahren zur Datenübertragung mit folgenden Schritten: Eingabe von ersten Daten aus einem stochastischen Prozess (114) in zumindest erste und zweite Teilnehmer (102, 104; 402, 404; 502, 504, 506, 508, 510, 512, 516) eines Kommunikationsnetzes (100, 106; 400, 406; 500, 514, 518), in jedem der zumindest ersten und zweiten Teilnehmer: Erzeugung eines symmetrischen Schlüssels (S1, S2), basierend auf den ersten Daten und Speicherung des symmetrischen Schlüssels für eine verschlüsselte Datenübertragung zwischen den zumindest ersten und zweiten Teilnehmern.